Background Paper BP-87E

COMPUTER CRIME

Monique Hébert
Marilyn Pilon
Law and Government Division

February 1984
Revised November 1991

Library of Parliament
Bibliothèque du Parlement

Research Branch

93-01845/

The Research Branch of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Research Officers in the Branch are also available for personal consultation in their respective fields of expertise.

©Minister of Supply and Services Canada 1992
Available in Canada through
your local bookseller
or by mail from
Canada Communication Group -- Publishing
Ottawa, Canada K1A OS9

Catalogue No. YM32-2/87-1991E
ISBN 0-660-14590-1

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

TABLE OF CONTENTS

Page

INTRODUCTION 1

DEFINITION OF COMPUTER CRIME 2

A. The Computer as Instrument 3

B. The Computer as Object 3
1. Data Diddling 4
2. Salami Techniques 5
3. Scavenging 5

THE SIGNIFICANCE OF COMPUTER CRIME 6

THE CANADIAN CONTEXT 8

PARLIAMENTARY ACTION 15

A. The Sub-Committee on Computer Crime 15

B. Legislative Response 16
1. *Criminal Law Amendment Act, 1985* 16
2. *An Act to Amend the Copyright Act*, S.C. 1988, c. 15 18

RECYCLED · RECYCLÉ

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

COMPUTER CRIME*

INTRODUCTION

Over the past 20 years the technology of electronic data processing - the computer - has come to play a dominant role in business and government. It would be difficult to conceive of a person whose life is not in some way affected by the computer, for virtually everyone who has a bank account, engages in any kind of credit transaction, or has dealings with the government or any large organization is touched in some way by the technology. The computer is now an indispensable tool for banking, corporate records and various activities of government.(1)

But the same features of the technology that make it such a boon to society at the same time increase its susceptibility to abuse. The absence of tangible printed records of credit transactions is testimony to the efficiency of the computer, yet it leaves the auditor without the accustomed "paper trail" with which accounts can be verified. A computer need not be manipulated at any particular place, but can be operated from a distance using telecommunications facilities. This too can increase the potential for abuse, for now a thief need not be anywhere near the site of the crime but can, from the relative safety of a computer terminal, acquire assets reduced to electronic impulses.

Losses attributed to criminal activities involving the use of computer systems are a subject of some controversy. No detailed study has ever been undertaken in Canada, in part because there is no consensus as to what exactly is a "criminal activity involving the use of computer systems." In any event, it is difficult to establish with any confidence

---

* This paper is based on work done by Donald MacDonald.

(1) T. Whiteside, *Computer Caper*, Crowell and Co., New York, 1978, p. 2.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

the losses from computer-crime without some clear conception of what such crime entails, and an accurate record of its frequency. Governments can have some effect on the former by defining which activities in relation to the computer are to be considered beyond acceptable standards of conduct. This may in turn have an effect on the degree to which computer abuse is reported.

DEFINITION OF COMPUTER CRIME

One very obvious question that arises in connection with the phrase "computer crime" is why should a certain area of conduct qualified by the adjective "computer" be fenced off for special consideration. We do not study filing cabinet crime, auto crime or television crime. Why should the instrument of the act make any difference? Is not theft still theft whether perpetrated with the use of break and enter tools or with a computer terminal?(2)

One response to this position is that the law is not only concerned with the prohibited ends of conduct, but also with the means used to attain those ends.

> The advent of the computer did not create a new crime, any more than the development of the automobile created a new form of larceny. As with the automobile, the criminal use of computer technology has increased the vulnerability of the community, and to the extent that the definition of crimes and the enactment of prohibitions is directed to the protection of the community, computer technology is a legitimate area of penal concern.(3)

Laws not only must enable the redress of wrongs or the punishment of the wrongdoer; they must also proscribe conduct; the complexity of the means for misconduct afforded by computer technology merits its special treatment.

---

(2) J. Becker, *The Investigation of Computer Crime*, U.S. Department of Justice, Washington, 1980, p. 1.

(3) D. Ingraham, "On Charging Computer Crime" (1980), 2 *Computer Law Journal*, 429.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHEQUE DU PARLEMENT

Thus, as the criminal law has been modified in some respects to take account of the automobile, so also will the computer engender changes. But beyond this, even more fundamental issues arise. A distinction must be made here between types of computer crime or abuse, between the computer as the "instrument" of crime and as the "object" of crime:

A. The Computer as Instrument

In these situations the computer is used as a means to an end. Here the criminal feeds false data into a computer in order to inflate the value of a cheque; or fiddles with an accounting program to cover up embezzlement; or forges bank deposit slips to gain an illicit windfall from customers who unknowingly use them to deposit money to the crimnal's account. In each case the thief uses the computer as the instrument of the crime. The means are novel, but the intent and the object are common - to acquire someone else's money without being entitled to it.

B. The Computer as Object

Where the computer is the instrument of crime we have familiar landmarks with which to identify the conduct as criminal. An individual whose intent is to get his or her hands on a tangible gain - money - uses the computer as a metaphorical pistol pointed at a bank teller. But where the computer is the object, things are not so clear. These situations, of course, are not limited to theft of the computer itself, but to those things associated with it which have substantial value but which are not tangible and whose legal status is unclear. For example, the information stored in a computer can be of inestimable value to its processor and to others and can be "stolen" without damage to the computer and without "depriving" the owner of its use. This applies to perhaps the most valuable information in a computer - the program - the key to how the machine carries out its data processing. And an even more intangible, yet valuable "thing" that can be taken is computer time. So great is the capacity of a computer and so valuable are its services that use of it even for short periods of time can be of great worth. The degree to which

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

these intangibles can or should be protected is a significant issue for the law.

This leads to a brief discussion of how computer crime is carried out. A computer has five principal component parts. First there is the input which converts data and instructions from human-readable to machine-readable codes. The central processing unit controls and coordinates the machines and the data based on its operating instructions, or program, also known as software. This is the heart of a cybernetic machine. All other processes are basically mechanical and repetitious, but made significant by the vast memory capacity and great speed of their operation, but software is qualitatively different - it governs how that data is to be processed. Next, the logical and memory units perform calculations, decision-making and storage functions in response to commands from the control unit. Finally, the output unit converts processing results back into human-readable language or symbols. A typical computer system may also use telecommunications facilities in order to link the central unit with terminals or printers located elsewhere.(4)

A computer system is vulnerable to invasion and abuse at virtually every component part. Personnel can alter data at the input stage; operations and systems programmers can manipulate data and software; transmission of data over common carrier lines can be tapped; and both authorized and unauthorized users can interfere with computer operations at terminals. The methods used to perpetrate theft or fraud by computer range from the ingenious to the banal. The following are some examples:

1. Data Diddling

This is described as "the simplest, safest, and most common method used in computer related crime."(5) Anyone who creates, records, transports, encodes, examines, checks or otherwise has access to data that will enter a computer has an opportunity to change that data to his or her

---

(4) Canada, *Changing Times: Banking in the Electronic Age*, Interdepartmental Steering Committee on the Electronic Payments System, Ottawa, 1979, p. 250.

(5) U.S. Department of Justice, Bureau of Justice Statistic, *Computer Crime - Criminal Justice Resource Manual*, Washington, D.C. 1979, p. 9.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

advantage before it enters processing. For example, a time clerk who filled out data forms for payroll purposes noticed that overtime claims were entered into the computer by employee number and not name. He accordingly put his number against the claims of other employees who worked overtime frequently, and received extra income over a period of time.(6)

2. Salami Techniques

This form of automated crime is so named because it involves stealing small amounts of assets from a large number of sources without noticeably reducing the whole. One form is the "round down" fraud. It involves alteration of the processing of bank interest calculations. Typically, interest calculations are rounded to the nearest cent and distributed among all accounts involved. The perpetrator modifies the program so that the remainder of all accounts rounded down are funnelled to an account over which he or she has control. Supposedly such a technique is virtually undiscoverable since customers would not notice the absence of fractions of a cent and auditors would not delve too deeply into such a program; although the return is not great, this crime would accumulate a tidy profit over time.(7)

3. Scavenging

This can be one of the less sophisticated forms of computer crime. It refers to the securing of information that may be left in or around a computer system after it has been used for a job. It can be as simple as searching trash barrels for copies of discarded computer listings or carbon papers from multiple-part forms used in input. In another example, time-sharing computers are involved. Frequently computer tapes are not erased but merely written over by the next user. A person seeking information can secure a tape used by a competitor, enter a small amount of data and read the entire tape back out, scavenging the information from the previous job.(8)

---

(6) *Ibid.*, p. 10. He was apprehended when an auditor noticed his unusually high income on a tax form and investigated further.

(7) *Ibid.*, p. 13-16.

(8) *Ibid.*, p. 23.

RECYCLED RECYCLE

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

The foregoing are just a few of the techniques used to perpetrate a computer-assisted crime. Many can be combatted through improved security and personnel evaluation and clearance methods. When theft or fraud is carried out by use of a computer the victim will usually eventually find out, because tangible property is being affected. But what of the "theft" of software or other information, or of computer services? This can be carried out, often without damage, instantaneously and without the owner's awareness. To prevent unauthorized use, code numbers, passwords and encryption devices are used. But these may be only as reliable as the personnel to whom they are divulged. The close association of various clients and businesses can vitiate these security devices(9) and there are techniques whereby access controls can be overridden by exploiting weaknesses in computer response to unauthorized attempts to breach its security.(10)

THE SIGNIFICANCE OF COMPUTER CRIME

The overall significance of computer crime is difficult to assess. Some contend that the statistics available are not reliable for such incidents because there is a more profound unwillingness to report computer-related crime than any other. One writer(11) has identified four reasons why discovered crimes are not reported or prosecuted:

1) the overall or imagined fear of the loss of public confidence;

2) the difficulty of proving that a crime has been committed;

3) concern about possible liability for lack of prevention of the incident;

---

(9) J.D. Parker, *Crime by Computer*, Scribner's, New York, 1976.

(10) Whiteside (1978), p. 115-126.

(11) S. Sokolik, "Computer Crime - The Need for Deterrent Legislation" (1980), 2 *Computer Law Journal* 353, at 359.

RECYCLED/RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

4) the user's belief that public exposure of the incident would be tantamount to an admission of vulnerability, as well as instruction to others on how to commit the crime.

Research has confirmed this unwillingness to publicize such incidents. The manager of a data processing division of a large corporation defrauded his employer by using $61,000 of computer time to operate his own computing business. The company declined to bring charges against him because it had already been a victim of a bigger fraud, which it did not want revealed. Another case involved a public utility company which "handled internally" a situation in which three employees had appropriated the company's computer system in order to trade on the commodities market.(12)

One body of opinion holds that computer abuse, even if widespread, should not be a matter of concern for legislators. According to this view, crime accomplished with the computer as instrument is fully prosecutable under existing substantive law (with perhaps some modification in procedural law, especially in rules of evidence). Other abuse, such as "theft" of information, or of computer time should be left to the civil law or innovation will be stifled.

One critic(13) contends that actual computer-assisted crime is much less prevalent than popularly believed and that a certain mystique has unfortunately attached to the whole area. He points to the celebrated *Rifkin* case in which a computer technician in California managed to have $10 million transferred from a bank computer to a Swiss bank account. The press characterized him as a "computer wizard" who had somehow manipulated the machine in some arcane way, when in fact he had done no more than steal a transfer code and impersonate a bank officer by telephone. His acts were prosecuted under existing penal law.(14) As for other computer crimes, the critic doubts the accuracy of reports of

---

(12) Canada, *Changing Times: Banking in the Electronic Age*, p. 253.

(13) J. Taber, "A Survey of Computer Crime Studies" (1980), 2 *Computer Law Journal* 275.

(14) For a full account see: J. Becker, "Rifkin, A Documentary History" (1980), 2 *Computer Law Journal* 471.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

incidents and holds, further, that some alleged "crimes" are, in a practical sense, impossible to commit. He contends, for example, that the "round down" computer fraud (see p. 5) is a myth, both impractical in view of existing banking procedures and logically incapable of bringing in more than miniscule returns.(15)

As for the security of computer systems, it is contended that this should not be an area for the penal sanction, but one in which users and owners should look out for their own interest by improving security and exercising civil remedies. The attachment of criminal consequences to unauthorized use could have serious effects on the computer industry. For example the common recreational and private use of "spare" computer time by programmers, operators and other users is regarded by many as a job perquisite akin to using a company telephone for limited personal calls. By making unauthorized access a crime such activities would be viewed as a theft of private property.(16)

Opponents of this laissez-faire view contend that the role of computer technology is so great and can affect so many people beyond its owners and direct users, that some form of legislative intervention is necessary. In addition, computer time and efficiency are so valuable that existing lax industry standards of security should no longer be tolerated.

THE CANADIAN CONTEXT

The distinction between computer as instrument and computer as object is useful in an analysis of Canadian criminal law respecting computers and the reforms of the 1980s.

Where the computer was used as the instrument of crime, there had been successful prosecutions under various provisions of the *Criminal Code*. A supervisor of accounts with a large company used a computer system to generate cheques payable to a fictitious company he

---

(15) Taber (1980), p. 311-327.

(16) R. Kling, "Computer Abuse and Computer Crime as Organisational Activities" (1980), 2 *Computer Law Journal* 403 at 406.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHEQUE DU PARLEMENT

had created by changing the numbers in invoices of regular customers. The cheques were sent to an accomplice, and the company lost over $100,000. The supervisor was convicted of fraud (section 338 of the Code) and sentenced to imprisonment. In another case, an employee of a stockbroker had permission to trade for his own account. He removed his trading losses from the employer's computer, manipulated balance figures after each day's dealings and doctored ledger books to make them balance also. In this way his losses could not be traced and were periodically written off. Over a period of six months he acquired between $65,000 and $100,000. He was subsequently convicted of theft and received a prison sentence of three years.(17) The major problem in such cases was not so much the application of substantive criminal law to the impugned conduct, as the detection and proof of the activities.(18)

Where the computer was the object of abuse, more serious problems arose because much of the conduct in this area was imperfectly dealt with by the *Criminal Code*, if at all.

A celebrated case took place at the University of Alberta in 1977. The computer system there, a substantial one serving the whole university community, was connected to over 300 terminals on campus, and also to telecommunication facilities. In the summer of 1977 the system was experiencing an unusual number of "crashes" or shutdowns of the system, up to five crashes in a week; more than one crash a week was considered

---

(17) Canada, *Changing Times: Banking in the Electronic Age*, p. 263, 266.

(18) In the case of *R.* v. *McMullen* (1979), 47 C.C.C. (2d) 499, the Ontario Court of Appeal held that in order for a computer printout to be entered as evidence it was necessary to prove the facts of the complete record-keeping process (i.e., input of entries, storage of information, and its retrieval and presentation). However, in *R.* v. *Bell and Bruce* (1982), 65 C.C.C. (2d) 377, the same court later held that computer printouts constituted "records" within the meaning of section 29(2) of the *Canada Evidence Act*, and, therefore, were admissible on the strength of affidavit evidence, a decision eventually affirmed by the Supreme Court of Canada (see *Bruce* v. *The Queen*, [1985] 2 S.C.R. 287). While there is little doubt that today's courts recognize the value of computer-produced evidence, it seems that clear standards of admissibility have yet to be developed; Kenneth L. Chasse, "Business Documents: Admissibility of Computer-Produced Records," *Crown Newsletter*, 1991, p. 27.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

unsatisfactory. It was determined that these were not being caused by equipment failure, but by improper programming. It was apparent that some unauthorized person was gaining access to the system, examining areas of batch data, interfering with the input of data, and acquiring other users' confidential passwords. University personnel monitored the system and, employing the computer's ability to identify the origin of its user, apprehended a student at one of the terminals. After an investigation it was determined that the student, Christensen, had been working closely with two others, McLaughlin and Astels. All three were charged with theft of telecommunication service:

> Everyone commits theft who fraudulently, maliciously, or without colour of right...
>
> (b) uses any telecommunication facility or obtains any telecommunication service.(19)

They were also charged with mischief:

> Everyone commits mischief who wilfully...
>
> (c) obstructs, interrupts or interferes with the lawful use enjoyment or operation of property.(20)

At trial, Astels was acquitted on both counts, owing to a reasonable doubt as to whether he had been informed that he was prohibited from using the computer; hence, he could plead "colour of right." Christensen, the student caught "red-handed," was convicted of both charges. The judge found that the computer could be considered a telecommunication facility within the definition in section 287(2):

> ... "telecommunication" means any transmission, emission, or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system.

The judge based his decision on the fact that the computer system was connected by telephone and coaxial cables to the telephone system and that there could be dial up connection through telephone lines to the central

---

(19) Section 287(1) of the *Criminal Code*.

(20) Section 387(1) of the *Criminal Code*.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

processing unit. The "crash" caused by Christensen had interfered with and interrupted the lawful use of university property and accordingly he was also guilty of mischief.(21) McLaughlin was also convicted under section 287. It was found that he had given Christensen programs and information and encouraged him to use the computer. He was thus found to be a party to the offence under section 20 of the Code in that he had aided and abetted the commission of the offence. He was acquitted of the mischief charge, however, because no evidence linked him with the "crash" which his friend had caused. He had aided in the theft but not the consequent mischief.

McLaughlin appealed his conviction on the ground that a computer system was not a "telecommunication facility." The Alberta Court of Appeal allowed the appeal,(22) and this decision was upheld by the Supreme Court of Canada on 18 July 1980. The Court ruled that although the computer system was connected to telephone facilities and was an electronic system, its function was not the transmission and reception of information, the hallmark of telecommunication. Rather, its *raison d'être* was data processing:

> ... the function of the computer is not the channelling of information to outside recipients so as to be susceptible in that respect to unauthorized use. Rather, it is to permit the making of complex calculations, to process and correlate information and to store it and enable it to be retrieved.(23)

Mr. Justice Estey added:

> Had Parliament intended to associate penal consequences with the unauthorized operation of a computer, it no doubt would have done so in a section of the *Criminal Code* or other penal statute in which the term which is now so permanently embedded in our language is employed. The court would not be expected by Parliament to glean from words generally associated with the communications industry an intent to attach penal consequences to the unauthorized operation of a computer.(24)

---

(21) *R.* v. *Christensen et al.* (1978), 26 *Chitty's Law Journal* 348, at 353.

(22) *R.* v. *McLaughlin* (1979), 12 C.R. (3d) 391.

(23) (1980), 18 C.R. (3d) 339, at 345, per Laskin, C.J.C.

(24) *Ibid.*, p. 349.

RECYCLED/RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

The decision caused something of a stir in the computer industry. It was interpreted to mean that there was nothing to prevent or deter anyone from making unauthorized use of computer facilities. This was not entirely true. It should be remembered that Christensen was convicted of "mischief," which can be treated as an indictable offence and carry up to a five-year sentence, for the "crash" he had caused. But it was questionable whether a mischief charge would stand for unauthorized access and use without a crash, for section 387 required obstruction and interruption of, or interference with a property owner. Conceivably, a skilled intruder could use a computer without directly contravening those prohibitions.

The *McLaughlin* case was the most detailed Canadian judicial treatment of issues related to the computer as the object of abuse, but there were other significant issues dealing with certain "intangibles" related to computers which existing Canadian criminal law did not clearly address. For example, information or data stored in a computer, particularly software or programs, can be extremely valuable. Such data can be taken in an instant, without damage to computer hardware, or without depriving the owner of the data store therein. Did taking computer data in itself constitute an offence under the *Criminal Code?*

That issue came before the courts in the case of *R.* v. *Stewart.*(25) The accused Stewart, a self-employed consultant, was charged with the offences of counselling theft and fraud when he attempted to obtain from a hotel security officer a copy of a computerized list of the names and addresses of the hotel's employees. The employee list was sought by the accused's client who wanted to organize the employees into a union.

Acquitted at trial, the accused was convicted on appeal. In a two-to-one decision, the Ontario Court of Appeal held that confidential information, such as a list of employees, came within the meaning of the terms "property" and "anything" as those terms are used in connection with

---

(25) *R.* v. *Stewart* (1982), 68 C.C.C. (2d) 305 (Ont. High Court); (1983), 35 C.R. (3d) 105 (Ont. Court of Appeal); (1988), 50 D.L.R. (4th) 1 (S.C.C.).

RECYCLED / RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

the offences of theft and fraud at sections 283 and 338 (now sections 322 and 380) of the *Criminal Code*.(26) Accordingly, the accused was guilty of both offences, although he could be convicted of only one since both counts flowed out of the same delict.

In his reasons for judgment, Mr. Justice Houlden held, on the one hand, that the accused was guilty of counselling a section 283(1)(d) theft, since had he been successful in obtaining the list, he would have dealt with the information in such a manner that it could not be returned to its owner, the hotel, in the same condition as it had been at the time of the taking, i.e., the information would have lost its "confidential" character. On the other hand, he found that for the offence of fraud it was sufficient to prove a risk of prejudice to the economic interests of the hotel; it was not necessary to show actual economic loss by reason of the fraud. Since the hotel could have sold its list of employees to promotional groups and therefore, could have profited from such a venture, the unauthorized taking of the list by the accused would have caused a risk of prejudice to the hotel's economic interests.

In a concurring judgment, Mr. Justice Cory added that although information *per se* was not property, there was a "right of property" in confidential information which came within the meaning of the term "property" at section 283(1). Citing copyright as an example of an enforceable proprietary interest, he held that the accused was guilty of counselling theft since he had sought to obtain from the security officer

---

(26) The relevant provisions of the *Criminal Code* stated:

283(1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate, with intent,

(a) to deprive, temporarily or absolutely, the owner of it or a person who has a special property or interest in it, of the thing or of his property or interest in it.

.....

(b) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

338(1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security [is guilty of an offence].

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

an unauthorized copy of the computerized list, thereby infringing the hotel's property interest in the list.

In a dissenting judgment, Mr. Justice Lacourcière would have sustained the acquittal on the ground that the term "anything" at section 283 had to be defined and qualified within the context of property, and that confidential information simply did not fit within that context. In his view, it was up to Parliament and not the courts to broaden the criminal definition of the property concept if the needs of Canadian society required it. Moreover, he felt that the mere loss to the hotel of the "confidentiality" of its information was not sufficiently prejudicial to its economic interests as to constitute a criminal fraud.

Mr. Stewart appealed his conviction for theft to the Supreme Court of Canada. If the majority judgment of the Ontario Court of Appeal had been sustained on appeal, it might have had far-reaching social implications, for what was at stake was not simply the attempted theft of a computerized list of employees, but more importantly, the broader issue of theft of information at large, regardless of its storage medium. Should information be treated as property, whether "confidential," "copyrightable" or otherwise? Was the criminal law an appropriate vehicle to sanction its misappropriation?

In a reversal of the Ontario Court of Appeal decision, the Supreme Court of Canada held that confidential information does not come within the meaning of the word "anything" in section 282 (now section 322) of the *Criminal Code*. To be the subject of theft, "anything" must be property in the sense that it has to belong to someone and it must be capable of being taken or converted in a manner that results in a deprivation of the victim. The Court found that confidential information does not constitute "property" for the purposes of the criminal law respecting theft and cannot *per se* be the subject of a taking, or of a conversion when the owner is not deprived of it.

Writing for a unanimous court, Mr. Justice Lamer also held that the nature of the information taken would not support a conviction for fraud, since the complainant had not been deprived of any money or economic advantage.

RECYCLED · RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

PARLIAMENTARY ACTION

A. The Sub-Committee on Computer Crime

On 9 February 1983, the subject-matter of Bill C-667, an Act to amend the *Criminal Code* and the *Canada Evidence Act* in respect of Computer Crime, was referred to the Standing Committee on Justice and Legal Affairs. The bill, introduced by the Hon. Perrin Beatty apparently in response to the legislative vacuum created by the *McLaughlin* case (the *Stewart* case had not come before the courts), sought, among other things, to (1) amend the definition of "property" in the *Criminal Code* to include computer software products, (2) create the offence of "computer theft" (the fraudulent diversion of a computer program to one's own or another person's use), and (3) expand the mischief provisions to encompass the unauthorized destruction, alteration or damage of computer programs.

In response to the order of reference, a Sub-committee on Computer Crime was established on 10 March 1983 with representation from the three parties. In the course of its hearings, the Sub-committee heard considerable evidence from a wide range of witnesses with expertise in such diverse fields as computer technology, security and management, computer law, the law of intellectual property, law enforcement, banking, privacy rights and consumer protection.(27) The Report of the Sub-committee on Computer Crime was tabled in the House of Commons on 29 June 1983.(28)

In its report, the Sub-committee agreed that the existing law was inadequate to deal with a number of computer-related abuses and concluded that, even though the incidence of computer crime in Canada was not known, there was a sufficient potential for serious harm to justify the enactment of criminal sanctions. However, the Sub-committee was not persuaded that the best way to proceed was expressly to include computer software products in the definition of "property." In its view, to treat computerized data as property might lead to more problems than it would

---

(27) *Minutes of Proceedings and Evidence* of the Sub-committee on Computer Crime of the Standing Committee on Justice and Legal Affairs, 32nd Parliament, 1st Session, 1980-81-82-83, Issues No. 1 to 17.

(28) *Ibid.*, Issue No. 18.

RECYCLED/RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

resolve, given the special status afforded information in our socio-legal system. Moreover, the Sub-committee felt that it would be inconsistent to proscribe the misappropriation of computerized data without, however, proscribing the misappropriation of information stored in other media.

For these reasons, the Sub-committee opposed the suggestion that the theft provisions of the *Criminal Code* be expanded expressly to cover the misappropriation of computerized information. Instead, it recommended the creation of two new offences prohibiting certain computer-related misconduct.

1) the unauthorized access (without colour of right) to a computer system; and

2) the unauthorized destruction and alteration (without colour of right) of computerized data.

The Sub-committee expressed the view that the enactment of criminal sanctions was but one way of discouraging computer-related abuses. Stressing the desirability of prevention over punishment, it recommended that the computer industry and institutional users adopt appropriate security measures, and that computer ethics be made an integral part of computer training. Moreover, finding that the misappropriation of computerized data could not be dealt with in isolation from the broader issue of information misappropriation, the Sub-committee concluded that a comprehensive approach to the problem had to be taken. In its view, legislative action was also needed to provide enhanced civil remedies to guard against information misappropriation and, therefore, recommended that other relevant laws (copyright, patent, trade secrecy, etc...) be examined and modified where necessary.

B. Legislative Response

1. *Criminal Law Amendment Act, 1985*

Criminal Code amendments dealing with computer crime came into effect on 4 December 1985. The various legislative provisions are substantially in keeping with the recommendations of the Sub-committee on

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

Computer Crime. On the one hand, unauthorized use of a computer is proscribed by section 342.1:

> (1) Everyone who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system.
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.
>
> (2) In this section,
>
> "computer program" means data representing instructions or statements that, when executed in a computer system, cause the computer system to perform a function;
>
> "computer service" includes data processing and the storage or retrieval of data;
>
> "computer system" means a device that, or a group of interconnected or related devices one or more of which,
>
> (a) contains computer programs or other data, and
> (b) pursuant to computer programs,
> (i) performs logic and control, and
> (ii) may perform any other function;
>
> "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

On the other hand, section 430 proscribes mischief in relation to data:

> (1.1) Everyone commits mischief who wilfully
>
> (a) destroys or alters data;
> (b) renders data meaningless, useless or ineffective;
> (c) obstructs, interrupts or interferes with the lawful use of data; or

RECYCLED · RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
>
> (5) Everyone who commits mischief in relation to data
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
> (b) is guilty of an offence punishable on summary conviction.
>
> (5.1) Everyone who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
> (b) is guilty of an offence punishable on summary conviction.
>
> (8) In this section, "data" has the same meaning as in section 342.1.

These measures avoid the problems that would have ensued from treating computerized data as property. By proscribing actions relative to, rather than focusing on ownership of, computerized data, the types of misconduct encountered in the *McLaughlin* and *Stewart* cases are effectively dealt with, without, however, venturing into the more dangerous zone of information ownership.

2. *An Act to Amend the Copyright Act*, S.C. 1988, c. 15

Also in keeping with the recommendations of the Sub-committee, were additional steps taken to address the issue of unauthorized appropriation of software materials. As a result of 1988 amendments to the *Copyright Act*, "computer program" is now defined and included in the definition of "literary works" protected under the Act. In addition to the civil remedies available for infringement of copyright, the Act makes it an offence punishable on summary conviction or indictment. Additional 1988 amendments increased the penalties for that offence to a maximum of one million dollars and/or five years' imprisonment, for conviction on indictment.

RECYCLED RECYCLÉ

Étude générale

BP-87F

LES DÉLITS INFORMATIQUES

Monique Hébert
Marilyn Pilon
Division du droit et du gouvernement

Février 1984
Révisé en novembre 1991

Bibliothèque du Parlement
Library of Parliament

Service de recherche

Le Service de recherche de la Bibliothèque du Parlement travaille exclusivement pour le Parlement, effectuant des recherches et fournissant des informations aux parlementaires et aux comités du Sénat et de la Chambre des communes. Entre autres services non partisans, il assure la rédaction de rapports, de documents de travail et de bulletins d'actualité. Les attachés de recherche peuvent en outre donner des consultations dans leurs domaines de compétence.

©Ministre des Approvisionnements et Services Canada 1992
En vente au Canada chez
votre libraire local
ou par la poste auprès du
Groupe Communication Canada -- Édition
Ottawa, Canada K1A OS9

N° de catalogue YM32-2/87-1991F
ISBN 0-660-93855-3

THIS DOCUMENT IS ALSO PUBLISHED IN ENGLISH

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

TABLE DES MATIÈRES

PAGE

INTRODUCTION..... 1

DÉFINITION DES DÉLITS INFORMATIQUES..... 2
A. L'ordinateur comme instrument du délit..... 3
B. L'ordinateur comme objet du délit..... 3
1. La falsification des données..... 5
2. Les techniques "salami"..... 5
3. La fouille..... 6

L'IMPORTANCE DES DÉLITS INFORMATIQUES..... 7

LE CONTEXTE CANADIEN..... 9

MESURES PARLEMENTAIRES..... 17
A. Sous-comité sur les infractions relatives aux ordinateurs. 17
B. Solutions législatives..... 19
1. *Loi de 1985 modifiant le droit pénal* 19
2. *Loi modifiant la Loi sur le droit d'auteur* 21

RECYCLED · RECYCLÉ

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

LES DÉLITS INFORMATIQUES*

INTRODUCTION

Depuis vingt ans, l'informatique et l'ordinateur se sont taillés une place importante dans les secteurs public et privé. On imagine difficilement une personne dont les activités ne seraient pas liées d'une façon ou d'une autre à l'ordinateur, car quiconque possède un compte en banque, effectue une transaction de crédit ou transige avec l'État ou n'importe quelle grande entreprise est touché par l'informatique. L'ordinateur est désormais un outil indispensable aux opérations bancaires, à l'archivage des sociétés et aux différentes activités de l'État(1).

Pourtant, les précieux avantages de l'informatique sont ceux-là même qui en multiplient les risques d'utilisation abusive. L'absence d'imprimés justifiant les opérations de crédit témoigne de l'efficacité de l'informatique, mais prive le vérificateur de toute preuve tangible qui lui permettrait de vérifier les comptes. Il n'est pas nécessaire d'être sur place pour manipuler un ordinateur puisqu'on peut le faire à distance grâce à des appareils de télécommunication. Ces progrès peuvent augmenter les risques d'abus, car désormais, le "pirate" peut opérer loin des lieux "du crime" et, avec la sécurité relative que lui procure un terminal informatique, acquérir des biens, qui sont réduits à des impulsions électroniques.

Le volume des pertes dues aux délits informatiques fait l'objet de controverse. Aucune étude approfondie n'a été faite à ce sujet au Canada, en partie parce qu'il n'y a pas de consensus sur la notion d'"infraction commise au moyen d'un ordinateur". Quoi qu'il en soit, il

---

* Ce document est inspiré d'une recherche effectuée par Donald MacDonald.

(1) T. Whiteside, *Computer Capers*, New York, Crowell and Co., 1978, p. 2.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

est difficile de recenser avec précision les pertes causées par ces délits sans avoir une conception claire de leur gravité, ni en connaître la fréquence exacte. Les gouvernements peuvent jouer un rôle en définissant les pratiques informatiques qui sont réputées contrevenir à l'éthique. Cette mesure pourrait, en retour, influer sur le nombre des délits informatiques signalés.

DÉFINITION DES DÉLITS INFORMATIQUES

À prime abord, on peut se demander pourquoi il est nécessaire de définir un code d'éthique particulier dans le cas des délits informatiques. On ne s'arrête pas aux délits associés à la manipulation de registres, à l'automobile ou à la télévision. Pourquoi l'instrument du délit ferait-il une différence? Un vol n'est-il pas toujours un vol, qu'il ait été commis par infraction ou à l'aide d'un terminal informatique(2).

On peut répondre à cela que le droit ne se préoccupe pas uniquement des fins illicites d'un acte, mais aussi des moyens utilisés pour les atteindre.

> L'avènement de l'informatique n'a pas créé de nouveaux délits, pas plus que celui de l'automobile n'a produit un nouveau type de vol. Tout comme dans le cas de l'automobile, l'utilisation criminelle de l'informatique a accru la vulnérabilité de la société et dans la mesure où la définition des délits et l'adoption de mesures législatives visant à interdire certains actes sont destinées à assurer la protection de la société, l'informatique est un champ de préoccupation légitime pour le droit pénal(3).

Les lois ne doivent pas seulement permettre le redressement des torts ou le châtiment des contrevenants; il leur est aussi essentiel de proscrire certains actes et la complexité des délits informatiques justifie qu'on leur accorde un traitement spécial.

---

(2) J. Becker, *The Investigation of Computer Crime*, Washington, département de la Justice des États-Unis, 1980, p. 1.

(3) D. Ingraham, "On Charging Computer Crime", *Computer Law Journal*, vol. 2, 1980, p. 429 (traduction).

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

De même que l'avènement de l'automobile a dicté des modifications au droit pénal, l'ordinateur imposera aussi des changements. L'informatique soulève pourtant des questions encore plus fondamentales. En effet, il faut distinguer entre les différents types de délits ou d'abus informatiques, c'est-à-dire entre ceux où l'ordinateur est "l'instrument" du délit et ceux où il en est "l'objet".

A. L'ordinateur comme instrument du délit

Dans ce cas, l'ordinateur est le moyen d'arriver à une fin. Par exemple, le contrevenant peut introduire de fausses données dans l'ordinateur pour augmenter la valeur d'un chèque qu'il doit recevoir, truquer un programme comptable pour couvrir un détournement de fonds ou falsifier des bordereaux de dépôt bancaire pour s'enrichir aux dépens de clients qui, sans le savoir, utilisent ces codes pour déposer de l'argent dans son compte. Dans chaque cas, le contrevenant utilise l'ordinateur comme instrument de son délit. Le moyen est nouveau, mais l'intention et la finalité du délit sont toujours les mêmes: s'approprier illégalement le bien d'autrui.

B. L'ordinateur comme objet du délit

Quand l'ordinateur est l'instrument du délit, nous disposons de paramètres connus nous permettant de qualifier l'acte de criminel. La personne dont l'intention est de se procurer un bien corporel, à savoir de l'argent, remplace le pistolet qu'elle pointerait sur la caissière par l'ordinateur. En revanche quand l'ordinateur est l'objet du délit, la situation n'est pas aussi claire. Ce genre de délit ne se borne pas, bien sûr, au vol d'un ordinateur comme tel, mais englobe tout bien incorporel qui lui est associé, dont la valeur est considérable mais le statut légal mal défini. Par exemple, l'information stockée en mémoire peut avoir une valeur inestimable pour son propriétaire et pour autrui, et un pirate peut se l'approprier sans causer de dommage apparent à l'ordinateur ni en priver son propriétaire. Ce genre de vol s'applique à l'information peut-être la plus précieuse que renferme l'ordinateur, à savoir le logiciel, clé du traitement des données. Il est également possible de s'emparer d'un "bien"

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

encore moins matériel mais d'une aussi grande valeur, le temps-machine. La capacité d'un ordinateur est tellement grande et ses services tellement utiles que son utilisation, même pour de courtes périodes, peut avoir beaucoup de prix. La question de savoir si ces biens incorporels peuvent ou doivent être protégés est importante sur le plan légal.

Ceci nous amène à discuter brièvement la façon dont sont commis les délits informatiques. Un ordinateur se compose de cinq éléments principaux. D'abord, il y a le périphérique d'entrée, qui convertit les données et les consignes conçues pour l'utilisateur en un code assimilable par la machine. Ensuite, vient l'unité centrale qui contrôle et coordonne ses fonctions et les données en faisant appel aux consignes d'exploitation ou programme, aussi appelé logiciel. Le logiciel est le coeur de la machine cybernétique; tous les autres procédés sont essentiellement mécaniques et répétitifs et leur valeur tient à la vaste capacité de la mémoire et à la rapidité de fonctionnement de la machine. Par contre, la valeur du logiciel est qualitative étant donné qu'il régit le traitement des données. Puis, il y a les unités de logique et de mémoire permettent à l'ordinateur d'effectuer des calculs, de prendre des décisions et de mémoriser les données, selon les consignes de l'unité de contrôle. Enfin, vient le périphérique de sortie qui convertit les résultats en un langage conçu pour l'utilisateur. L'unité centrale d'un ordinateur type peut également, grâce à des appareils de télécommunication, être reliée à des terminaux et à des imprimantes situés à distance(4).

Chaque élément de l'ordinateur est susceptible de faire l'objet d'abus. Les employés peuvent fausser les données à entrer, les programmeurs de fonctions et d'étude peuvent manipuler les données et le logiciel, il est possible de prélever les données pendant leur transmission, et les utilisateurs de terminaux, autorisés, ou non, peuvent intervenir pendant l'exécution des opérations-machine. Les méthodes utilisées pour commettre un vol ou un délit informatique peuvent être ingénieuses ou banales. En voici quelques exemples.

---

(4) Canada, *Changing Times: Banking in the Electronic Age*, Ottawa, Comité directeur interministériel des systèmes de paiements électroniques, 1979, p. 250.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

1. La falsification des données

Il s'agit de l'infraction la plus simple, le plus sûre et la plus courante(5). Quiconque introduit, mémorise, transmet, code, examine ou vérifie des données informatiques, ou y a accès d'une façon quelconque, a la possibilité de les modifier à son avantage avant leur traitement. Citons, à titre d'exemple, le cas du commis chargé de remplir des formules de données pour la paye, qui avait remarqué que les demandes de compensation des heures supplémentaires étaient introduites dans l'ordinateur en fonction du numéro et non du nom de l'employé. Il lui a suffi d'inscrire son propre numéro sur les demandes d'employés qui faisaient souvent des heures supplémentaires pour toucher un revenu supplémentaire pendant un certain temps(6).

2. Les techniques "salami"

On les désigne ainsi parce qu'elles ont pour but de voler de petites quantités de biens à partir d'un grand nombre de sources sans réduction apparentée de l'ensemble. La falsification des sommes à arrondir en est un exemple. Elle consiste à fausser le calcul des intérêts bancaires. Habituellement, les intérêts sont arrondis au cent et répartis entre tous les comptes concernés. Le fraudeur modifie donc le programme pour que la fraction de cent de tous les comptes dont les sommes ont été arrondies soit acheminée dans un autre compte, qu'il contrôle. Apparemment, ce délit passe pratiquement inaperçu étant donné que les clients sont peu susceptibles de remarquer l'absence des fractions de cent et le vérificateur pousse rarement aussi loin son étude du programme; et même si la valeur du vol n'est pas énorme, elle finit par représenter une somme rondelette avec le temps(7).

---

(5) Département de la Justice des États-Unis, Bureau de la Statistique de la Justice, Washington (D.C.), *Computer Crime - Criminal Justice Resource Manual*, 1979, p. 9.

(6) *Ibid.*, p. 10. Il a été appréhendé quand un vérificateur, alerté par le revenu anormalement élevé inscrit sur sa formule d'impôt, a décidé de mener une enquête poussée.

(7) *Ibid.*, p. 13-16.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

3. La fouille ---

C'est l'une des formes de délit informatique les moins complexes. Elle consiste à se procurer des renseignements laissés dans ou près de l'ordinateur après utilisation. Le contrevenant peut tout simplement fouiller dans les corbeilles à papier pour y trouver des listes d'ordinateur ou des copies carbone de données mémorisées. Il peut aussi profiter de l'exploitation en temps partagé d'ordinateurs pour commettre ce genre de délit. Comme habituellement on n'efface pas les bandes pour ordinateur mais qu'on superpose tout simplement les nouvelles données aux anciennes, quiconque cherche de l'information peut se procurer la bande d'un concurrent, y entrer quelques données et la relire au complet pour y recueillir des renseignements déjà mémorisés(8).

Ce ne sont là que quelques-unes des techniques dont les pirates se servent pour perpétrer des délits informatiques. Il est possible de prévenir un grand nombre de ces délits par des mesures de sécurité accrues, une évaluation serrée du personnel et l'utilisation de méthodes de contrôle sécuritaire. Le vol ou la fraude commis au moyen d'un ordinateur seront tôt ou tard décelés puisqu'il y a eu atteinte aux biens matériels de la victime. Par contre, qu'en est-il du "vol" de logiciel ou d'autres renseignements, ou même de services informatiques? Ce genre de délit peut souvent être commis instantanément sans dommage apparent, et à l'insu du propriétaire. Afin de prévenir l'accès non autorisé aux renseignements informatisés, on utilise des codes, des mots de passe et des dispositifs de chiffrage; toutefois, la fiabilité de ces mesures de sécurité dépend largement du personnel qui est mis dans le secret. D'une part, les liens étroits qui unissent les divers clients et entreprises risquent de compromettre la sécurité de ces mécanismes(9) et, d'autre part, il existe certaines techniques qui permettent d'outrepasser ces moyens de contrôle en exploitant les faiblesses de l'ordinateur face aux tentatives de violation des mesures de sécurité(10).

---

(8) *Ibid.*, p. 23.

(9) D. Parker, *Crime By Computer*, New York, Scribner's, 1976.

(10) Whiteside, (1978), p. 115-126.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

L'IMPORTANCE DES DÉLITS-INFORMATIQUES

Il est difficile d'évaluer l'importance globale des délits informatiques. Certains maintiennent qu'on ne peut se fier aux statistiques disponibles sur ce genre d'incidents puisqu'il existe, dans ce secteur en particulier, une très forte réticence à signaler les délits commis. Un auteur(11) a établi quatre raisons qui expliquent ce phénomène:

1) la crainte, justifiée ou non, de perdre la confiance du public;

2) la difficulté de prouver qu'un tel crime a été commis;

3) la peur d'être tenu responsable de ne pas avoir su prévenir l'incident;

4) la crainte qu'en rendant l'affaire publique, l'utilisateur reconnaisse, par le fait même, sa vulnérabilité et expose, au vu et au su de tous, des façons de tromper le système.

Le recherches entreprises dans le domaine ont confirmé qu'il existe au Canada la même réticence à rendre public ce genre d'incidents. Prenons, par exemple, le cas d'un gestionnaire de la division du traitement des données d'une importante société commerciale, qui avait fraudé son employeur de quelque 61 000 $, en utilisant l'ordinateur de la société aux fins d'exploitation de sa propre entreprise. Or, la société a refusé de porter plainte contre lui, ayant déjà été victime d'une fraude plus grave sur laquelle elle ne désirait pas attirer l'attention. De la même façon, une société de services publics a décidé de "régler de façon interne", le cas de trois de ses employés qui avaient décidé "d'emprunter" le système informatisé de la société, pour spéculer sur le marché des produits de base(12).

---

(11) S. Sokolik, "Computer Crime - The Need for Deterrent Legislation", *Computer Law Journal*, vol. 2, 1980, p. 353-359.

(12) Canada, *Changing Times: Banking in the Electronic Age*, p. 253.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

D'aucuns maintiennent que les délits informatiques, même s'ils sont assez répandus, ne devraient pas préoccuper les législateurs; ils sont plutôt d'avis que les infractions commises au moyen d'un ordinateur sont déjà assujetties à des lois existantes bien structurées, sous réserve de quelques modifications qui pourraient être apportées sur le plan de la procédure, particulièrement en ce qui concerne le droit de la preuve. Par ailleurs, les autres délits, tels le "vol" de renseignements, ou de temps-machine relèvent, à leur avis, du droit civil, puisque l'adoption d'une lourde réglementation risquerait d'étouffer l'esprit d'innovation.

De l'avis d'un critique(13), les infractions perpétrées au moyen d'un ordinateur sont en réalité beaucoup moins répandues qu'on ne le croit généralement, et un certain mythe s'est créé autour des délits informatiques. Il cite, à titre d'exemple, la célèbre affaire *Rifkin*, dans laquelle un technicien en information de la Californie est parvenu à faire porter dix millions de dollars à son compte en Suisse, au moyen de l'ordinateur d'une banque. La presse a présenté Rifkin comme une espèce de "génie informatique" qui aurait manipulé l'ordinateur de façon très mystérieuse, alors qu'en réalité il n'avait fait que "voler" un code de transfert et usurper l'identité d'un cadre de la banque lors d'une conversation téléphonique. L'affaire a fait l'objet d'une poursuite aux termes des dispositions existantes du droit pénal(14). Pour ce qui est des autres délits informatiques, le même auteur met en doute la véracité de certains rapports d'incidents et affirme que certains "crimes" qui sont réputés avoir été commis se révèlent, dans la pratique, irréalisables. Il maintient, par exemple, que la fraude informatique par falsification des sommes à arrondir (expliquée plus haut) n'est qu'un mythe étant à la fois irréalisable dans la pratique bancaire actuelle et logiquement incapable de rapporter davantage que des profits dérisoires(15).

---

(13) J. Taber, "A survey of Computer Crime Studies", *Computer Law Journal*, vol. 2, 1980, p. 275.

(14) Pour un récit plus détaillé voir: J. Becker "Rifkin, A Documentary History", *Computer Law Journal*, vol. 2, 1980, p. 471.

(15) Taber (1980), p., 311-327.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

En ce qui concerne la sécurité des systèmes informatiques, certains estiment qu'il n'y a pas lieu de prévoir de sanctions pénales à cet égard, et qu'il incombe plutôt aux utilisateurs et aux propriétaires de surveiller leur propre intérêt en améliorant les mesures de sécurité et en instaurant certaines méthodes de réglementation. Le fait de considérer l'utilisation non autorisée des ordinateurs comme un acte criminel risquerait d'avoir de graves incidences sur l'industrie de l'informatique. Par exemple, nombreux sont ceux qui considèrent l'usage, par les programmeurs, opérateurs et autres utilisateurs, du temps-machine libre à fins récréatives ou personnelles comme un privilège d'emploi assez semblable à l'utilisation limitée du réseau téléphonique de l'employeur pour des appels personnels. En tenant l'utilisation non autorisée pour un délit criminel, ce genre d'activités serait alors considéré comme un vol de la propriété privée(16).

Les adversaires de cette politique de laissez-faire font valoir l'extrême importance de la technologie informatique et ses répercussions éventuelles sur une foule d'autres personnes que les propriétaires et utilisateurs directs pour justifier une certaine forme d'intervention juridique. Ils maintiennent en outre que le temps-machine et l'efficacité du système représentent une valeur telle que les normes de sécurité qui ont actuellement cours dans ce secteur industriel à être sérieusement resserrées.

LE CONTEXTE CANADIEN

La distinction entre d'ordinateur comme instrument et comme objet du délit se révèle utile pour une analyse du droit pénal en matière d'informatique et des réformes qui y ont été apportées dans les années 80.

De nombreuses poursuites intentées aux termes des dispositions du *Code criminel* ont pu être menées à bien dans des cas où l'ordinateur avait été utilisé comme instrument du délit. Par exemple, le

---

(16) R. Kling, "Computer Abuse and Computer Crime as Organizational Activities", *Computer Law Journal*, vol. 2, 1980, p. 403-406.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

superviseur de la comptabilité d'une importante société commerciale avait utilisé un système informatique pour libeller des chèques à l'ordre d'une société fictive qu'il avait créée en changeant les numéros de facture des clients réguliers. Les chèques étaient ainsi acheminés à un complice, et la société a perdu plus de 100 000 $. Le superviseur a été reconnu coupable de fraude aux termes de l'article 338 du Code et condamné à une peine d'emprisonnement. Dans un autre cas, un employé d'une firme de courtage pourvu de l'autorisation de négocier à son propre compte avait pu effacer ses pertes de l'ordinateur de l'employeur, manipuler son solde à la fermeture des transactions quotidiennes, et fausser les grands livres en conséquence. Ainsi, ses pertes ne pouvaient être retracées et se trouvaient périodiquement effacées. Sur une période de six mois, il a réussi à usurper entre 65 000 et 100 000 $. L'employé en question a par la suite été reconnu coupable de vol et condamné à une peine de trois ans d'emprisonnement(17). Le principal problème que pose ce genre d'affaire concerne non pas l'application des dispositions du droit pénal comme telles, mais plutôt la détection des activités frauduleuses et la preuve(18).

---

(17) Canada, *Changing Times: Banking in the Electronic Age*, p. 263 et 266.

(18) Dans l'affaire *R.* c. *McMullen* (1979), 47 C.C.C. (2d) 499, la Cour d'appel de l'Ontario a posé, comme condition à la recevabilité des imprimés d'ordinateurs en preuve, l'obligation de faire état des étapes du processus intégral de tenue des dossiers (c.-à-d. la saisie des données, ainsi que le stockage, l'extraction et la présentation de l'information); en revanche, le même tribunal a par la suite décidé, dans l'affaire *R* c. *Bell and Bruce* (1982), 65 C.C.C. (2d) 377, que les imprimés d'ordinateurs constituaient des "registres" aux termes du paragraphe 29(2) de la *Loi sur la preuve au Canada* et qu'ils étaient, par conséquent, recevables en preuve. Ce jugement a par la suite été confirmé par la Cour suprême du Canada *(Bruce* c. *La Reine*, [1985] 2 R.C.S. 287). Sans doute que les tribunaux d'aujourd'hui reconnaîtraient la recevabilité des éléments de preuve informatiques. Il n'en demeure pas moins que ces normes de recevabilité restent à définir. Kenneth L. Chasse, "Business Documents: Admissibility of Computer-Produced Records", *Crown Newsletter*, 1991, p. 27.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

Par contre, les cas d'usage abusif de l'ordinateur comme objet du délit posent des problèmes beaucoup plus difficiles à résoudre, puisque le *Code criminel* ne comporte à cet égard que des dispositions imparfaites, sinon inexistantes.

Un cas très célèbre s'est présenté à l'Université de l'Alberta, en 1977. L'important système informatique qui dessert toute la communauté universitaire était relié à 300 terminaux sur le campus et à un certain nombre d'installations de télécommunications. Au cours de l'été 1977, le système a subi un nombre démesurément élevé de pannes, (jusqu'à 5 pannes par semaine) qui ont par la suite été attribuées non pas à une défectuosité du matériel, mais bien à une mauvaise programmation. Avec plus d'une panne par semaine, le rendement de l'ordinateur aurait déjà été jugé insatisfaisant. Il était évident qu'une personne avait accès au système sans autorisation. Le pirate était en mesure d'utiliser un multiprocesseur, il pouvait intervenir dans la saisie des données et obtenir les mots de passe confidentiels d'autres utilisateurs. Le personnel de l'université a entrepris de surveiller le système et, grâce à l'ordinateur, il a pu déterminer l'origine de ces activités et appréhender un étudiant à l'un des terminaux. L'enquête a révélé que l'étudiant en question, un certain Christensen, travaillait en étroite collaboration avec deux collègues, McLaughlin et Astels. Tous trois ont été accusés de fraude du service de télécommunications:

> Commet un vol quiconque, frauduleusement, malicieusement ou sans apparence de droit,
>
> b) se sert d'un fil ou câble de télécommunication ou obtient un service de télécommunication(19).

Par ailleurs, ils ont également été accusés de méfait:

> Commet un méfait, quiconque, volontairement,
>
> c) empêche, interrompt ou gêne l'emploi, la jouissance ou l'exploitation légitime d'un bien(20).

---

(19) Paragraphe 287(1) du *Code criminel*.

(20) Article 387(1) du *Code criminel*.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

Au cours du procès, Astels a été acquitté des deux chefs d'accusation, en raison du doute raisonnable qui subsistait quant à savoir s'il avait été mis au courant de l'interdiction d'utiliser l'ordinateur; il a donc pu invoquer "l'apparence de droit." Par contre, Christensen, l'étudiant qui avait été pris en flagrant délit, a été reconnu coupable des deux chefs d'accusation. Le juge a déclaré que l'ordinateur pouvait être assimilé à une "installation de télécommunication", aux termes de la définition formulée au paragraphe 287(2):

> [...] "télécommunication" signifie toute transmission, émission ou réception de signes, signaux, écrits, images ou sons ou de renseignements de toute nature par fil ou câble.

Le juge a fondé sa décision sur le fait que le système informatique était relié au réseau téléphonique au moyen d'un câble téléphonique et d'un câble coaxial, et que les lignes téléphoniques pouvaient être mises en communication avec l'ordinateur central. La "panne" occasionnée par Christensen avait interrompu l'usage légal de la propriété de l'université et, par conséquent, ce dernier a également été reconnu coupable de méfait(21). McLaughlin a par ailleurs été inculpé aux termes de l'article 287. Apparemment, il aurait fourni à Christensen les programmes et l'information nécessaires, et l'aurait encouragé à utiliser l'ordinateur. Il a donc été reconnu complice de l'infraction commise aux termes de l'article 20 du Code, ayant aidé à la perpétrer. Il a toutefois été acquitté de l'accusation de méfait, puisque le tribunal n'a pu prouver son accusation en rapport avec la "panne" occasionnée par son ami. Il aurait donc aidé au vol, mais non pas au méfait qui s'en est suivi.

McLaughlin a interjeté appel de sa condamnation, arguant qu'un système informatique n'est pas une "installation de télécommunication". La Cour d'appel de l'Alberta a accueilli l'appel(22) et sa décision a été entérinée par la Cour suprême du Canada le 18 juillet 1980. Cette dernière a jugé que même si le système informatique était relié au

---

(21) *R.* c. *Christensen et al.* (1978), *Chitty's Law Journal,* vol. 26, p. 348-353.

(22) *La Reine* c. *McLaughlin* (1979), 12 C.R. (3d) 391.

RECYCLED PAPER

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

réseau téléphonique et qu'il constituait un système électronique, il ne servait pas à la transmission et à la réception de l'information qui caractérisent les télécommunications. L'ordinateur a plutôt comme raison d'être le traitement de données:

> [...] L'ordinateur n'a pas pour fonction d'acheminer des renseignements vers des points extérieurs, auquel cas il pourrait se prêter à une utilisation non autorisée. Il sert plutôt à faire des calculs complexes, à traiter, mettre en corrélation, emmagasiner et extraire des données(23).

Le juge Estey a ajouté:

> Si le Parlement avait voulu associer des sanctions pénales à l'utilisation non autorisée d'un ordinateur, il l'aurait exprimé dans un article du *Code criminel* ou dans une autre loi en recourant à cette expression dont l'emploi est devenu courant. Le Parlement ne s'attendait certainement pas à ce que le tribunal glane dans la terminologie généralement employée dans l'industrie des télécommunications l'intention de lier des sanctions pénales à l'utilisation non autorisée d'un ordinateur(24).

La décision a causé un certain remous dans l'industrie informatique qui l'a interprétée comme signifiant qu'il n'existe aucun moyen d'empêcher ou de dissuader quelqu'un d'utiliser un ordinateur sans autorisation. Ce n'est pas tout à fait vrai. Il faut se rappeler que pour la panne qu'il avait provoquée, M. Christensen a été reconnu coupable de méfait, infraction punissable par voie de mise en accusation et capable de valoir une peine maximale d'emprisonnement de cinq ans. Mais il est douteux qu'une accusation de méfait puisse être portée dans le cas d'une utilisation non autorisée n'ayant causé aucune panne puisque, aux termes de l'article 387, il faut empêcher, interrompre ou gêner l'exploitation d'un bien par son propriétaire. Il est possible qu'une personne habile utilise un ordinateur sans contrevenir à ces interdictions.

---

(23) (1980), 18 C.R. (3d) p. 339-345, par Laskin, J.C.

(24) *Ibid.*, p. 349.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

L'affaire *McLaughlin* a donné lieu au jugement le plus détaillé au Canada en matière d'usage abusif d'un ordinateur à titre d'objet de l'infraction, mais il est d'autres aspects importants concernant certains biens non matériels reliés aux ordinateurs sur lesquels le droit pénal canadien est vague. Par exemple, l'information ou les données emmagasinées dans un ordinateur peuvent avoir une grande valeur, en particulier le logiciel ou les programmes. Ces données peuvent être prises instantanément, sans dommage apparent à l'ordinateur ou à l'insu de leur propriétaire qui n'en est pas privé. Le fait de s'emparer de données informatisées constitue-t-il en soi une infraction au *Code criminel?*

Cette question a été débattue devant les tribunaux. Dans l'affaire *La Reine* c. *Stewart* (25), le prévenu, un expert-conseil indépendant, a été accusé d'incitation au vol et à la fraude parce qu'il avait tenté d'obtenir d'un gardien de sécurité d'un hôtel une copie de la liste informatisée des noms et adresses des employés de l'hôtel. Le client de l'accusé voulait utiliser cette liste pour syndiquer les employés.

Acquitté par le tribunal de première instance, l'accusé a été reconnu coupable en appel. Dans une décision à deux contre un, la Cour d'appel de l'Ontario a jugé que les renseignements confidentiels, comme une liste d'employés, constituaient un "bien" et une "chose quelconque" au sens des articles 283 et 338 du *Code criminel* (qui portent maintenant les numéros 322 et 380)(26), qui régissent les infractions de vol et de

---

(25) *La Reine* c. *Stewart* (1982), 68 C.C.C. (2d) 305 *(Ontario High Court);* (1983), 35 C.R. (3d) 105 *(Ontario Court of Appeal);* (1988), 50 D.L.R. (4e) 1, C.S.C.

(26) Les dispositions pertinentes du *Code criminel* stipulent:
283(1) Commet un vol, quiconque prend frauduleusement et sans apparence de droit, ou détourne à son propre usage ou à l'usage d'une autre personne, frauduleusement et sans apparence de droit, une chose quelconque, animée ou inanimée, avec l'intention,
a) de priver, temporairement ou absolument, son propriétaire, ou une personne y ayant un droit de propriété spécial ou un intérêt spécial, de cette chose ou de son droit ou intérêt dans cette chose.
[...]

(suite à la page 15)

RECYCLED · RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

fraude. L'accusé était donc coupable des deux infractions, mais il ne pouvait être condamné que pour une seule puisque les deux chefs d'accusation émanaient du même délit.

Dans les attendus de son jugement, le juge Houlden a déclaré d'une part que l'accusé était coupable d'avoir conseillé un vol aux termes de l'alinéa 238(1)d) puisque s'il avait réussi à obtenir la liste, il aurait agi de telle manière à l'égard des renseignements qu'elle contenait qu'il lui aurait été impossible de les rendre à leur propriétaire, l'hôtel, dans leur état d'origine; en d'autres mots, les renseignements auraient perdu leur caractère "confidentiel". D'autre part, pour ce qui est de la fraude, il suffisait de prouver qu'il y avait risque de préjudice aux intérêts économiques de l'hôtel et qu'il n'était pas nécessaire de faire la preuve qu'il y avait eu des pertes concrètes à cause de la fraude. Puisque l'hôtel aurait pu vendre sa liste d'employés à des groupes de promotion publicitaire et tirer profit d'une telle affaire, l'utilisation non autorisée de la liste par l'accusé aurait pu nuire à ses intérêts économiques.

Dans un jugement concordant, le juge Cory a ajouté que même si les renseignements ne constituent pas un bien en soi, il existe un "droit de propriété" applicable à l'information confidentielle qui découle du sens de l'expression "propriété" au paragraphe 283(1). Citant les droits d'auteur comme exemple de droit de propriété reconnu par la loi, le juge a soutenu que l'accusé était coupable d'incitation au vol puisqu'il avait tenté d'obtenir d'un agent de sécurité, sans autorisation, une copie de la liste informatisée, portant ainsi atteinte aux droits de propriété de l'hôtel sur cette liste.

Dans un jugement dissident, le juge Lacourcière aurait maintenu l'acquittement en portant que l'expression "chose quelconque" à

---

(26) suite de la page 14:

> b) d'agir à son égard de telle manière qu'il soit impossible de la remettre dans l'état où elle était au moment où elle a été prise ou détournée.
>
> 338(1) Est coupable d'un acte criminel quiconque, par la supercherie, le mensonge ou d'autres moyens dolosifs, constituant ou non un faux semblant au sens de la présente loi, frustre le public ou toute personne, déterminée ou non, de quelque bien, argent ou valeur.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

l'article 283 devait être définie et qu'elle s'appliquait dans le contexte de la propriété, contexte où les renseignements confidentiels n'avaient pas leur place. À son avis, il revient au Parlement et non aux tribunaux d'étendre, au criminel, la définition de propriété si l'intérêt de la société l'exige. En outre, le juge a estimé que la seule perte par l'hôtel du caractère "confidentiel" des renseignements ne constituait pas une atteinte suffisante à ses intérêts économiques pour constituer une fraude.

M. Stewart a interjeté appel de sa condamnation pour vol devant la Cour suprême du Canada. Si celle-ci avait confirmé le jugement majoritaire de la Cour d'appel de l'Ontario, cette décision aurait pu avoir des répercussions sociales importantes, car l'enjeu n'était pas simplement la tentative de vol d'une liste mécanographique d'employés, mais, surtout le vol de renseignements en général, indépendamment de la nature du stockage. L'information doit-elle être considérée comme un bien, qu'il s'agisse d'information de nature confidentielle, protégée par des droits d'auteurs ou autres? Le *Code criminel* était-il l'instrument approprié pour sanctionner leur détournement?

Renversant la décision de la Cour d'appel de l'Ontario, la Cour suprême du Canada a statué que l'expression "chose quelconque" employée dans l'article 282 du *Code criminel* (maintenant l'article 322) n'englobe pas ce type d'information confidentielle. Pour que l'appropriation d'une "chose quelconque" puisse être considérée comme un vol, la chose volée doit être un bien sur lequel quelqu'un a un droit de propriété et elle doit pouvoir lui être enlevée ou être détournée de manière à l'en fruster. La Cour a conclu que ce type d'information confidentielle n'est pas un bien assorti d'un "droit de propriété" aux fins de l'application des dispositions du droit criminel concernant le vol. En soi, cette chose ne peut être enlevée ou détournée si son propriétaire n'en est pas privé.

Dans son arrêt, le juge Lamer, qui a rédigé le jugement unanime, a également soutenu qu'à cause de la nature de l'information prise, il ne saurait être question de fraude, car le plaignant n'a été frustré ni d'argent ni d'avantages économiques.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

MESURES PARLEMENTAIRES

A. Sous-comité sur les infractions relatives aux ordinateurs

Le 9 février 1983, le principe du projet C-667, Loi modifiant le *Code criminel* et la *Loi sur la preuve au Canada* en ce qui concerne les infractions contre les droits de propriété relatifs aux ordinateurs, a été renvoyé au Comité permanent de la justice et des questions juridiques. Ce projet de loi d'initiative parlementaire a apparemment été présenté pour remédier aux lacunes législatives mises en évidence par l'affaire *McLaughlin* (les tribunaux n'avaient pas encore été saisis de l'affaire *Stewart);* il visait, entre autres, à modifier la définition de "bien" ou "propriété" dans le *Code criminel* pour y inclure les produits du logiciel informatique, à créer l'infraction de "vol de logiciel ou de données informatiques" (le détournement frauduleux d'un programme d'ordinateurs pour son propre usage ou celui d'une autre personne), et à étendre les dispositions concernant le méfait à la destruction et à l'altération non autorisées de programmes d'ordinateur et aux dommages causés à de tels programmes.

À la suite de l'ordre de renvoi, un Sous-comité sur les infractions relatives aux ordinateurs, composé de représentants des trois partis politiques, a été créé le 10 mars 1983. Pendant les audiences, le Sous-comité a entendu les dépositions d'un grand nombre de témoins spécialisés dans des domaines aussi variés que les techniques informatiques, la sécurité et la gestion, le droit de l'information, le droit de la propriété intellectuelle, l'application de la loi, les pratiques bancaires, le droit en matière de protection de la vie privée et de protection du consommateur(27). Le rapport du Sous-comité sur les infractions relatives aux ordinateurs a été déposé à la Chambre des communes le 29 juin 1983(28).

---

(27) *Procès-verbaux et témoignages* du Sous-comité sur les infractions relatives aux ordinateurs du Comité permanent de la justice et des questions juridiques, 32e législature, première session, 1980-1981-1982-1983, fascicules nos 1 à 17.

(28) *Ibid.*, fascicule n° 18.

RECYCLED/RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

Dans son rapport, le Sous-comité reconnaissait que le droit existant ne régissait pas efficacement un certain nombre de délits reliés à l'informatique et concluait que même si on ne connaissait pas l'ampleur de ce type de criminalité au Canada, il existait suffisamment de possibilités de préjudices graves pour justifier l'adoption de sanctions pénales. Toutefois, le Sous-comité n'était pas convaincu que la meilleure solution consistait à assortir de droits de propriété les produits du logiciel informatique. À son avis, l'application aux données informatisées de la notion de "bien" pourrait entraîner davantage de problèmes qu'elle n'en résoudrait compte tenu de la place de premier plan qu'occupe l'information dans notre système socio-juridique. En outre, le Sous-comité estimait qu'il serait illogique d'interdire le prélèvement de données stockées sur ordinateur sans interdire aussi le prélèvement de données consignées par d'autres méthodes.

Ces considérations ont amené le Sous-comité à s'opposer à ce que les dispositions du *Code criminel* concernant le vol soient étendues explicitement au détournement de données informatisées. Par contre, il a recommandé la création de deux nouvelles infractions correspondant à certains actes dans le domaine de l'informatique.

1) l'utilisation non autorisée d'un système informatique (sans apparence de droit); et
2) la modification ou la destruction non autorisées (sans apparence de droit) de données informatisées.

Le Sous-comité a estimé que l'adoption de sanctions pénales n'était qu'une des façons possibles de prévenir les infractions dans le domaine de l'informatique. Il a insisté sur le rôle prépondérant de la prévention par rapport à la répression en recommandant que les sociétés de services informatiques et les institutions qui se servent d'ordinateurs adoptent les mesures de sécurité qui s'imposent, et que l'éthique fasse partie intégrante de la formation en informatique. Constatant par ailleurs que le détournement de données informatisées était inséparable de la question plus générale du détournement de renseignements, le Sous-comité en a conclu que le problème devait être abordé globalement. À son avis, il faudrait prendre des mesures législatives pour favoriser les recours au civil pour prévenir les détournements de renseignements; c'est pourquoi le Sous-comité a recommandé que les lois applicables en la matière (concernant

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

notamment le droit d'auteur, les brevets, le secret industriel, etc...) soient réévaluées et modifiées au besoin.

B. Solutions législatives

1. *Loi de 1985 modifiant le droit pénal*

Les modifications législatives apportées au *Code criminel* sont entrées en vigueur le 4 décembre 1985. Elles s'inspirent substantiellement des recommandations du Sous-comité sur les infractions relatives aux ordinateurs. D'une part, l'utilisation non autorisée d'un ordinateur est interdite par l'article 342.1, qui dispose:

> 342.1(1) Quiconque, frauduleusement et sans apparence de droit:
> a) directement ou indirectement, obtient des services d'ordinateur;
> b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;
> c) directement ou indirectement utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa a) ou b) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur,
> est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.
>
> (2) Les définitions qui suivent s'appliquent au présent article. [...]
>
> "ordinateur": Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux:
> a) contiennent des programmes d'ordinateur ou d'autres données;
> b) conformément à des programmes d'ordinateur:
> (i) soit exécutent des fonctions logiques et de commande,
> (ii) soit peuvent exécuter toute autre fonction.
>
> "programme d'ordinateur": Ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction.

RECYCLED RECYCLÉ

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

> "service d'ordinateur": S'entend notamment du traitement des données de même que la mémorisation et du recouvrement ou du relevé des données.

D'autre part, l'article 430 proscrit le méfait concernant des données en ces termes:

> (1.1.) Commet un méfait quiconque volontairement, selon le cas:
> a) détruit ou modifie des données;
> b) dépouille des données de leurs sens, les rend inutiles ou inopérantes;
> c) empêche, interrompt ou gêne l'emploi légitime des données;
> d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit. [...]
>
> (5) Quiconque commet un méfait à l'égard de données est coupable:
> a) soit d'un acte criminel et passible d'un emprisonnement maximal de dix ans;
> b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.
>
> (5.1) Quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données est coupable:
> a) soit d'un acte criminel et passible d'un emprisonnement maximal de cinq ans;
> b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire. [...]
>
> (8) Au présent article, "données" s'entend au sens de l'article 342.1.

Ces mesures permettent d'éviter les problèmes qui auraient pu résulter du fait de traiter les données informatiques comme des biens auquel peut être rattaché un droit de propriété. En insistant sur l'interdiction de poser certains actes relatifs aux données informatiques, plutôt que sur leur propriété, il devient effectivement possible de se prononcer sur le genre de méfaits commis dans les affaires *McLaughlin* et *Stewart* sans toutefois s'aventurer dans l'aspect plus délicat de la propriété de l'information.

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

2. *Loi modifiant la Loi sur le droit d'auteur*, L.C. 1988, c. 15

Également dans l'esprit des recommandations du Sous-comité, d'autres mesures ont été prises concernant l'appropriation non autorisée du matériel informatique. Depuis les modifications apportées à la *Loi sur le droit d'auteur* en 1988, la définition d'"oeuvres littéraires" englobe les "programmes d'ordinateur", de sorte que ceux-ci sont par le fait même protégés. Or, en plus de permettre des recours civils, la Loi considère l'atteinte aux droits d'auteur comme un délit punissable sur déclaration de culpabilité par procédure sommaire ou par voie de mise en accusation. En outre, dans les deux cas, les peines imposées pour ce genre de délit peuvent maintenant atteindre un million de dollars et cinq ans d'emprisonnement.